SAFETY AND SECURITY ASSURANCE - CALL FOR REVIEW
13 January 2004

Introduction

Organizations within the US Federal Aviation Administration (FAA) and the US Department of Defense (DoD) are sponsoring a joint effort with the objective of identifying best safety and security practices for process improvement and appraisal use in combination with the two integrated capability maturity models:

- FAA integrated Capability Maturity Model® (FAA-iCMM® or iCMM) version 2.0 (available at www.faa.gov/ipg), and
- Capability Maturity Model Integration® for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI®-SE/SW/IPPD/SS or CMMI) version 1.1 (available at www.sei.cmu.edu)

This project is co-managed by the Chief Engineer for Process Improvement in the FAA and the Deputy Director for Software Assurance in DoD, with broad participation from government, industry and the Software Engineering Institute.

We have progressed to the point where we are requesting a second external review of the set of practices that have been developed by the project team, and their proposed placement in relation to CMMI and iCMM. Your participation is much appreciated!

Instructions for Reviewers

This package includes the following information in 4 files:

1. In this file: A. Safety and Security Assurance - Project Overview
   B. Safety and Security Assurance Application Area - Overview
   C. Application Area – Description and Considerations
   D. Work Environment Process Area - Overview
   E. Project Team Roster
2. Safety and Security Assurance Application Area, including goals, practices, notes, and preliminary glossary
3. Work Environment Process Area
4. Change Request Form

Please let us know your opinions regarding any aspect of this package including both the safety and security specific content, and its proposed use in relation to CMMI and iCMM.

Submission: Please complete your review using the Change Request Form provided and submit your comments by **Monday, 1 March 2004** to Curt Wells at cw@i-metrics.net

For further information regarding this project see www.faa.gov/ipg, or if you wish to participate in pilot safety and security assurance appraisals, please contact:

Linda Ibrahim, PhD
Chief Engineer for Process Improvement
Office of the Assistant Administrator for
Information Services and Chief Information Officer
Federal Aviation Administration
Email: Linda.Ibrahim@faa.gov
Phone: 202-267-7443

or

Joe Jarzombek, PMP
Deputy Director for Software Assurance
Information Assurance Directorate
Office of Assistant Secretary of Defense
(Networks and Information Integration)
Email: Joe.Jarzombek@osd.mil
Phone: 703-627-4644

We thank you in advance for your valued participation in this critical project.
Linda and Joe

A. Safety and Security Assurance – Project Overview

Project Description: Organizations within the US Federal Aviation Administration (FAA) and US Department of Defense (DoD) are sponsoring a joint effort with the objective of identifying best safety and security practices for use in combination with the two integrated CMMs: FAA-iCMM v2.0, and CMMI V1.1.

Why it is important: Safety and security are critical to DoD and FAA, as well as other government and industry organizations. Both CMMI and iCMM provide process improvement frameworks in which safety and security activities can take place. Yet some practices specific to safety and security are not necessarily addressed in these models. The FAA approved a project to include both safety and security in the iCMM, and the CMMI Steering Group had discussed addressing safety and security. In light of similar needs, FAA and DoD decided to collaborate on developing safety/security extensions to both iCMM and CMMI, the intent being that common content would be included in both models.

Who has been involved: This project is being co-managed by FAA Chief Engineer for Process Improvement and Deputy Director for Software Assurance in DoD, with broad participation from government and industry. The team comprises over 30 participants from FAA, DoD, Army, Navy, Air Force, NASA, Department of Energy, Australian Defence Materiel Organization, Defense Contract Management Agency, Software Engineering Institute, Northrop Grumman, Lockheed Martin, Computer Sciences Corp., Harris Corp., I-Metrics, and Praxis Critical Systems Ltd (UK). In addition, many individuals and organizations have participated as reviewers, and in safety and security pilot appraisals.

What has been produced so far:

- Source Material selected by experts from safety and security communities of practice to be integrated and incorporated comprising three safety standards and four security standards.
  For safety: *MIL-STD-882C:* System Safety Program Requirements
  IEC 61508: Functional Safety of Electrical/ Electronic/ Programmable Electronic Systems
  DEF STAN 00-56: Safety Management Requirements for Defence Systems
  For security: *ISO 17799:* Information Technology - Code of practice for information security management
  ISO 15408: The Common Criteria (v 2.1) Mapping of Assurance Levels and Families
  ISO/IEC 21827: Systems Security Engineering (SSE) CMM (v2.0)
  NIST 800-30: Risk Management Guide for Information Technology Systems
- Integrated practices for safety, and integrated practices for security, developed and synthesized from the source standards, retaining mappings of all synthesized practices to the source material.
- Harmonization of the safety and security components resulting in combined practices (with mappings retained) that were distributed for external review.
- Disposition of over 200 comments on initial draft package received from ~35 reviewers from US, Australia, and various European countries.
- Pilot appraisals – two in the FAA and one in a company, others planned for initiation.
- Packaging of reviewed/revised practices into an appropriate form for integration with the existing practices of the reference models. This packaging consists of a Safety and Security Assurance Application Area, and a Work Environment Process Area as described in this review package.
- Distribution of package for second external review. **This is where we are now!**

What's next:

- Revision/finalization based on reviewers' comments and pilot appraisal results
- Publication and incorporation for use with iCMM and CMMI

Who would use this:
It is expected that these practices will be utilized for process improvement in several contexts: strategically to support enterprise-wide safety and security work; in any program/organization that deals with safety and security assurance of products and services; by those groups responsible for a safe and secure work environment; and by acquisition programs in evaluating the capability of suppliers to deliver safe and secure products and services.

B. Safety and Security Assurance Application Area - Overview

Safety and Security Assurance Application Area
This Application Area (AA) identifies standards-based application practices (APs) expected to be used as criteria in guiding process improvement and in appraising an organization's capabilities for providing safe and secure products and services. These application practices are used in conjunction with Capability Maturity Model Integrated (CMMI) or the FAA integrated Capability Maturity Model (iCMM).

Purpose – The purpose of Safety and Security Assurance is to establish and maintain a safety and security capability, define and manage requirements based on risks attributable to threats, hazards, and vulnerabilities, and assure that products and services are safe and secure.

AA Goal 1 – An infrastructure for safety and security is established and maintained.

AP01.01. Ensure safety and security awareness, guidance, and competency.

AP01.02. Establish and maintain a qualified work environment that meets safety and security needs.

AP01.03. Establish and maintain storage, protection, and access and distribution control to assure the integrity of information.

AP01.04. Monitor, report and analyze safety and security incidents and identify potential corrective actions.

AP01.05. Plan and provide for continuity of activities with contingencies for threats and hazards to operations and the infrastructure.

AA Goal 2 – Safety and security risks are identified and managed.

AP01.06. Identify risks and sources of risks attributable to vulnerabilities, security threats, and safety hazards.

AP01.07. For each risk associated with safety or security, determine the causal factors, estimate the consequence and likelihood of an occurrence, and determine relative priority.

AP01.08. For each risk associated with safety or security, determine, implement and monitor the risk mitigation plan to achieve an acceptable level of risk.

AA Goal 3 – Safety and security requirements are satisfied.

AP01.09. Identify and document applicable regulatory requirements, laws, standards, policies, and acceptable levels of safety and security.

AP01.10. Establish and maintain safety and security requirements, including integrity levels, and design the product or service to meet them.

AP01.11. Objectively verify and validate work products and delivered products and services to assure safety and security requirements have been achieved and fulfill intended use.

AP01.12. Establish and maintain safety and security assurance arguments and supporting evidence throughout the lifecycle.

AA Goal 4 – Activities and products are managed to achieve safety and security requirements and objectives.

AP01.13. Establish and maintain independent reporting of safety and security status and issues.

AP01.14. Establish and maintain a plan to achieve safety and security requirements and objectives.

AP01.15. Select and manage products and suppliers using safety and security criteria.

AP01.16. Measure, monitor and review safety and security activities against plans, control products, take corrective action, and improve processes.

B. Safety and Security Assurance Application Area - Overview

This Application Area is to be used in conjunction with the Capability Maturity Model Integration (CMMI) or the FAA integrated Capability Maturity Model (iCMM).

As with Process Areas in the CMMI and the iCMM, generic practices are applied to the Application Area to guide process improvement and to support appraisal of capabilities. The generic practices of iCMM and CMMI are depicted below:

Capability Level	iCMM Generic Practices	CMMI Generic Practices
Level 1	1.1 Identify the Work Scope 1.2 Perform the Process	1.1 Perform Base Practices
Level 2	2.1 Establish Organizational Policy 2.2 Document the Process 2.3 Plan the Process 2.4 Provide Adequate Resources 2.5 Assign Responsibility 2.6 Ensure Skill and Knowledge 2.7 Establish Work Product Requirements 2.8 Consistently Use and Manage the Process 2.9 Manage Work Products 2.10 Objectively Assess Process Compliance 2.11 Objectively Verify Work Products 2.12 Measure Process Performance 2.13 Review Performance with Higher-level Mgmt 2.14 Take Corrective Action 2.15 Coordinate With Participants & Stakeholders	2.1 Establish an Organizational Policy 2.2 Plan the Process 2.3 Provide Resources 2.4 Assign Responsibility 2.5 Train People 2.6 Manage Configurations 2.7 Identify and Involve Relevant Stakeholders 2.8 Monitor and Control the Process 2.9 Objectively Evaluate Adherence 2.10 Review Status with Higher Level Management
Level 3	3.1 Standardize the Process 3.2 Establish and Use a Defined Process 3.3 Improve Processes	3.1 Establish a Defined Process 3.2 Collect Improvement Information
Level 4	4.1 Stabilize Process Performance	4.1 Establish Quantitative Objectives for Process 4.2 Stabilize Subprocess Performance
Level 5	5.1 Pursue Process Optimization	5.1 Ensure Continuous Process Improvement 5.2 Correct Root Causes of Problems

B. Safety and Security Assurance Application Area - Overview

For application practices, this Safety and Security Assurance Application Area draws upon implementing practices in the relevant process areas (PAs) in the CMMI and the iCMM as depicted in the following table. Where indicated, material from the iCMM would be adopted for use in the CMMI. It is anticipated that a future release of CMMI will incorporate practices required for implementing safety and security assurance application practices.

iCMM PAs	**CMMI PAs** ***(including practice extensions taken from iCMM)***	**Provides implementing practices to Safety and Security (S&S) Assurance AA Application Practices (short name titles)**
PA 22 Training	Organizational Training	AP01.01 Ensure S&S Competency
PA 19 Work Environment	Work Environment	AP01.01 Ensure S&S Competency AP01.02 Establish Qualified Work Environment AP01.05 Ensure Business Continuity
PA 17 Information Management	*Information Management* *(PA 17 extended from iCMM)*	AP01.03 Control Information
PA 10 Operation and Support	*Operation and Support* *(PA 10 extended from iCMM)*	AP01.04 Monitor Incidents
PA 13 Risk Management	Risk Management	AP01.05 Ensure Business Continuity AP01.06 Identify S&S Risks AP01.07 Analyze and Prioritize Risks AP01.08 Determine, Implement & Monitor Risk Mitigation Plan AP01.14 Establish a S&S Plan
PA 00 Integrated Enterprise Management	Organizational Environment for Integration Organizational Innovation and Deployment *Integrated Enterprise Management* *(PA 00 extended from iCMM)*	AP01.05 Ensure Business Continuity AP01.09 Identify Regulatory Requirements, Laws & Standards AP01.13 Establish Independent S&S Reporting AP01.14 Establish a S&S Plan AP01.16 Monitor & Control Activities and Products
PA 01 Needs PA 02 Requirements	Requirements Development Requirements Management	AP01.09 Identify Regulatory Requirements, Laws & Standards AP01.10 Establish S&S Requirements and Design
PA 03 Design	Technical Solution	AP01.10 Establish S&S Requirements and Design
PA 08 Evaluation	Verification Validation	AP01.11 Objectively Evaluate Products AP01.12 Establish S&S Assurance Argument
PA 15 Quality Assurance and Management	Process and Product Quality Assurance	AP01.12 Establish S&S Assurance Argument AP01.13 Establish Independent S&S Reporting AP01.16 Monitor and Control Activities and Products
PA 11 Project Management	Project Planning Project Monitoring and Control Integrated Project Management Quantitative Project Management	AP01.13 Establish Independent S&S Reporting AP01.14 Establish a S&S Plan AP01.16 Monitor and Control Activities and Products
PA 16 Configuration Management	Configuration Management	AP01.16 Monitor and Control Activities and Products
PA 18 Measurement and Analysis	Measurement and Analysis	AP01.16 Monitor and Control Activities and Products
PA 05 Outsourcing PA 12 Supplier Agreement Mgmt PA 09 Deployment, Transition, & Disposal	Supplier Agreement Management Integrated Supplier Management	AP01.15 Select & Manage Suppliers, Products & Services
PA 21 Process Improvement	Organizational Process Focus	AP01.16 Monitor and Control Activities and Products

C. Application Area – Description and Considerations

What is an application area?
An application area (AA) is a construct proposed for use with both iCMM and CMMI reference models. An AA groups together related application practices (APs) that are considered essential for achieving the requisite outcomes particular to the application or discipline. The application practices are implemented by performing practices that are already in process areas of the reference model, with explicit guidance derived from source standards. Thus, application areas provide a guide for identifying which selected process areas and practices in a reference model need to be implemented to address the purpose of the application area. The application practices also provide additional interpretive guidance for ways that the practices in the reference model might be implemented in the particular context of the application.

Why are only safety and security addressed?
An Application Area could be developed for another discipline, and indeed others are being considered to help in focusing appraisals and process improvement using the continuous representation of the reference models. For now, safety and security have been considered because of their importance in government and industry. Moreover, this focus has enabled a better harmonization of practices between the two disciplines.

How does this Safety and Security Assurance AA relate to safety and security standards?
The application area proposed in this review package is the Safety and Security Assurance application area. The application practices in this AA are the harmonized safety and security practices that were synthesized from the source standards identified by subject matter experts in the safety and security communities of practice. The source standards that were selected represent those in community-wide use, and those standards with industry-specific guidance would be accommodated via the application practice (AP) "identify and document applicable regulatory requirements, laws, standards, policies, and acceptable levels of safety and security." (see further discussion of standards below)

Why aren't these harmonized practices being proposed as CMMI "amplifications" or iCMM "notes" in relation to the existing practices?
In order to make the practice of safety and security in organizations explicitly improvable and appraisable, the safety and security application practices need to be structured as "expected" practices. The informative nature of amplifications and notes does not meet this need. Simply adding informative material to existing practices in the reference models provides no assurance that safety and security would be included in process improvement or appraisal of capabilities. The AA also provides direct visibility, in a single location, to those practices needed for safety and security assurance.

Why are these harmonized safety and security assurance application practices being proposed as an application area (AA), rather than a new process area (PA)?
The harmonized safety and security assurance application practices are already addressed in a more general fashion in reference model existing practices, without sufficient explicit consideration for safety or security concerns. To introduce new practices that are already addressed, though generally, in the reference models would be confusing and would be largely redundant. Also, the harmonized application practices do not offer the breadth and depth of reference model practices regarding practice implementation details.

How is an application area constructed?
An application area is similar to a process area since it contains a purpose statement, goals (application goals), and expected practices (application practices). Application goals reflect outcomes to be achieved for the application area to be considered successfully implemented. They are useful in establishing process improvement objectives, and are required components for appraisal purposes. Application practices are mapped to goals, and they are the activities that, when performed, are expected to result in achievement of those goals. Application practices are implemented, however, by performing the indicated practices in the reference models, as interpreted by the information, derived from the source standards, provided in the application practice.

C. Application Area – Description and Considerations

How is an application area appraised?
The Standard CMMI Appraisal Methodology for Process Improvement (SCAMPI), the FAA iCMM Appraisal Method (FAM), and other Appraisal Requirements for CMMI (ARC) Class A appraisal methods can be applied to application areas by employing the generic practices of either iCMM or CMMI. Thus an AA could be appraised at any capability level. The goals of the application area would be used in appraisal, and the practices mapped to those goals would be the implementation practices in the reference models, considered in the context of the interpretative guidance provided in the AA. In an AA stand-alone appraisal, only the AA goals need to be considered, if that is the desired scope. Of course ARC Class B and C appraisals could also be used to gain an understanding of process capabilities relative to safety and security.

How would organizations or individuals use the safety and security assurance application area?
It is expected that these practices will be used for process improvement in several contexts: strategically, to support enterprise-wide safety and security work; in any program/organization that deals with safety and security assurance of products and services; by those groups responsible for a safe and secure work environment; and by acquisition programs in evaluating the capability of suppliers to deliver safe and secure products and services.

How does use of the Safety and Security Assurance Application Area relate to System/Product Certification/Accreditation and Acceptance Testing?
The Safety and Security Assurance AA complements (but does not replace) Certification/Accreditation and Acceptance Testing of Systems and Products because the AA includes requisite practices, which if implemented, should contribute to the delivery of safe and secure products and services, and more readily support achievement of Certification/Accreditation expected outcomes.

How does the Safety and Security Assurance Application Area relate to other standards?

- The National Institute of Standards and Technology (NIST) implements guidelines responsive to Public Law 104-106 (Clinger-Cohen Act of 1996) and OMB Circular A-130. Other related standards and publications have not been explicitly referenced in this AA; however, as written, this Safety and Security Assurance AA lends itself to full support of the NIST 800-series pubs that provide an organization with further tools for bolstering their security processes. NIST issued the Oct 2003 draft of "Recommended Security Controls For Federal Information Systems," NIST Special Publication 800-53, which details controls the government will require in 2005 and is expected to influence controls to be used by other governments and business (csrc.nist.gov/publications/drafts.html). Security controls are the management, operational, and technical safeguards and countermeasures prescribed for a computer system that, taken together, adequately protect the confidentiality, integrity, and availability of a system and its information:
  - Management safeguards range from risk assessment to security planning.
  - Operational safeguards include factors such as personnel security and hardware and software maintenance.
  - Technical safeguards include audit trails and communications protection.

- The Federal Information Security Management Act contains guidelines about establishing security standards and requirements for information and information systems, including business process improvement and states "Federal agencies should follow NIST guidelines, if applicable and whenever feasible."

C. Application Area – Description and Considerations

- ISO/IEC 15026:1997, System and Software Integrity Levels, was used by the Harmonization Team as a basis for harmonizing terminology and concepts between the safety and security communities. ISO/IEC JTC1/SC7 WG9, is the international working group that produced this Standard, and includes members of both communities. WG9 is in the process of redefining its terms of reference to include *development of standards and technical reports for system and software assurance. System and software assurance addresses management of risk and assurance of safety, security, and dependability within the context of system and software life cycles*. WG9 is also in the process of revising 15026 and will continue to collaborate in the development and maintenance of this AA.

- Useful discussions have taken place with the UK Ministry of Defence (MoD) and Praxis Critical Systems regarding the SafSec Project, a research study on Integrating Safety and Security for Integrated Modular Avionics, funded by UK MoD. The synergy with the SafSec project lies in the similar aims of combining safety and security for improved effectiveness. The SafSec project deliverables are currently under consideration by UK MoD, and are expected to be finalized in March 2004.

How does the safety and security assurance application area relate to industry-specific regulatory guidance?

Standards and laws that provide more detailed industry-specific guidance for safety and security would be addressed within this Safety and Security Assurance AA via the application practice AP01.09 to "Identify and document applicable regulatory requirements, laws, standards, policies, and acceptable levels of safety and security." For example, RTCA DO-178B would be required for avionics systems and software.

D. Work Environment Process Area - Overview

The new Work Environment Process Area provides details of what is to be accomplished to "Establish and maintain a qualified work environment that meets safety and security needs" (AP 01.02). Note that this process area is not specific to safety and security assurance, and it could be used for other applications or disciplines.

Purpose: The purpose of the Work Environment process area is to ensure that people have working procedures and infrastructure to meet stakeholder needs.

Goal: A work environment that meets stakeholder needs is established and maintained.

Practices:

01 Establish and maintain the needs and requirements to implement, operate and sustain work environments.

02 Establish and maintain a description of work environment standards and tailoring guidelines that meet identified needs and requirements.

03 Establish and maintain a work environment, tailored from the work environment standards, to meet the specific needs.

04 Maintain the required qualification of work environment components.

05 Ensure that personnel have the required competencies and qualifications to access, use, and maintain the work environment.

06 Monitor, evaluate and insert, as appropriate, new technology for improving the work environment.

07 Plan and provide for continuity of the work environment.

E. Safety and Security Assurance Project Team Members

Name	Organization	Team/Role
Ahern, Dennis	Northrop Grumman Electronic Systems	Model Team
Ashford, Matt	Australian Defence Materiel Organisation (DMO)	Safety Co-lead
Bate, Roger	Software Engineering Institute	Model Team
Coblentz, Brenda	US Department of Energy (DOE)	Safety Team Pilot Team
Conrad, Ray	Lockheed Martin Air Traffic Management (Safety)	Safety Team Pilot Team
Cooper, David	Praxis Critical Systems Ltd (UK)	Harmonization Team
Courington, Tim	FAA/Northrop Grumman Mission Systems	Security Co-lead
Croll, Paul	Computer Sciences Corp	Harmonization Team Lead
Dhami, Sartaj	Northrop Grumman Mission Systems	Security Team
Gill, Janet	US Navy, NAVAIR Software System Safety Lead	Safety Team
Henning, Ronda	Harris Corp	Security Co-lead
Horn, Mary	US Federal Aviation Administration (FAA)	Security Team
Ibrahim, Linda	US Federal Aviation Administration (FAA)	Project Co-Manager Model Team Lead Pilot Team
Jackson, Tom	Lockheed Martin	Security Team
Jarzombek, Joe	US Office of Secretary of Defense (OSD)	DoD Co-Sponsor Project Co-Manager Harmonization Team
Keblawi, Faisal	US Federal Aviation Administration (FAA)	Security Co-Lead
Kemens, Victor	US Federal Aviation Administration (FAA)	Security Team
LaBruyere, Larry	FAA/Northrop Grumman Mission Systems	Pilot Team Lead
Leonette, Martha J.	US Federal Aviation Administration (FAA)	Security Team
Miller, Gerald	FAA/Northrop Grumman Mission Systems	Security Team
Ming, Lisa	Defense Contract Management Agency	Safety Team
Patel, Raju B.	US Air Force, Wright Patterson AFB	Security Team
Pierson, Hal	US Federal Aviation Administration (FAA)	Security Team
Pyster, Art	US Federal Aviation Administration (FAA)	FAA Co-Sponsor
Roseboro, Douglas	US Federal Aviation Administration (FAA)	Security Team
Sherer, Wayne	US Army, Picatinny Arsenal	Model Team
Simmons, Marty	Lockheed Martin Mission Systems (Security)	Security Team
Stroup, Ron	US Federal Aviation Administration (FAA)	Safety Co-lead
Stuart, Sandra	US Federal Aviation Administration (FAA)	Security Team
Terry, Ray C	US Navy, NAVAIR Systems Safety Division Head	Safety Team
VanBuren, Scott	US Federal Aviation Administration (FAA)	Harmonization Team
Wells, Curt	I-Metrics LLC	Model Team
Wetherholt, Martha	NASA	Safety Team